Mobile Configuration Profiles for iOS Devices

Technical Note

Mobile Configuration Profiles for iOS Devices Technical Note

December 10, 2013

04-502-197517-20131210

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2013-03-27	Initial Release.
2013-12-10	Updated for FortiClient (iOS) v5.0 Patch Release 2.

Introduction

The purpose of this document is to provide instructions on how to create a mobile configuration profile, specifically the VPN and Global HTTP proxy payloads.

The document also covers how to upload the mobile configuration to your FortiGate device, and how to deploy this profile via the endpoint control feature to registered FortiClient (iOS) v5.0 Patch Release 1 or later devices.

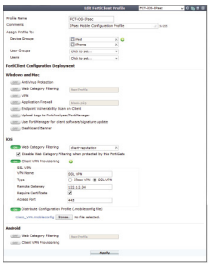
This document covers the iPhone Configuration Utility and the Apple Configurator app for mobile configuration profile creation. The mobile configuration can include the following: IPsec configuration to your FortiGate, global HTTP proxy configuration to use your FortiGate as a web proxy server for mobile internet traffic, and restrictions to enable greater control of client use of company iOS devices.

Create, upload, and deploy a .mobileconfig profile to clients

The following figure illustrates the steps required to create, upload, and deploy a `.mobileconfig` profile to registered clients to use the built-in IPsec VPN client on your iOS device. The endpoint control feature in FortiOS allows you to distribute the `.mobileconfig` file to FortiClient iOS devices for centralized management and control of these devices.

Figure 1: Deploy mobile configuration to iOS devices

1 Configure your mobile configuration profile using the iPhone Configuration Utility, the Apple Configurator app, or Lion Server Profile Manager and export the .mobileconfig file.



2 Upload the .mobileconfig file to a FortiOS FortiClient Profile. Use the FortiOS Endpoint Control feature to push the profile to registered FortiClient iOS devices.

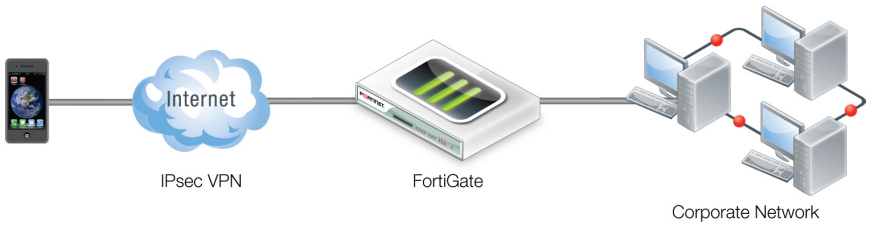
3 The user installs the FortiClient Profile pushed from the FortiGate device to their FortiClient iOS device. FortiClient iOS is required to install the .mobileconfig file to the iOS device.

4 The user can connect to the FortiGate using the IPsec configuration and configured in the .mobileconfig profile. If configured, FortiClient iOS will use the FortiGate as a web proxy server.

Example 1: Configure an IPsec VPN connection to your FortiGate

The FortiClient iOS app does not currently support IPsec VPN. You can use the Cisco IPsec VPN client which is built into your iOS device to connect to a FortiGate device. You can configure this VPN client in the iOS configuration profile, upload the profile to your FortiGate device, and deploy the configuration profile to your managed iOS device using the FortiGate endpoint control feature. FortiClient iOS does not participate in the IPsec VPN connection, but is required for endpoint control.

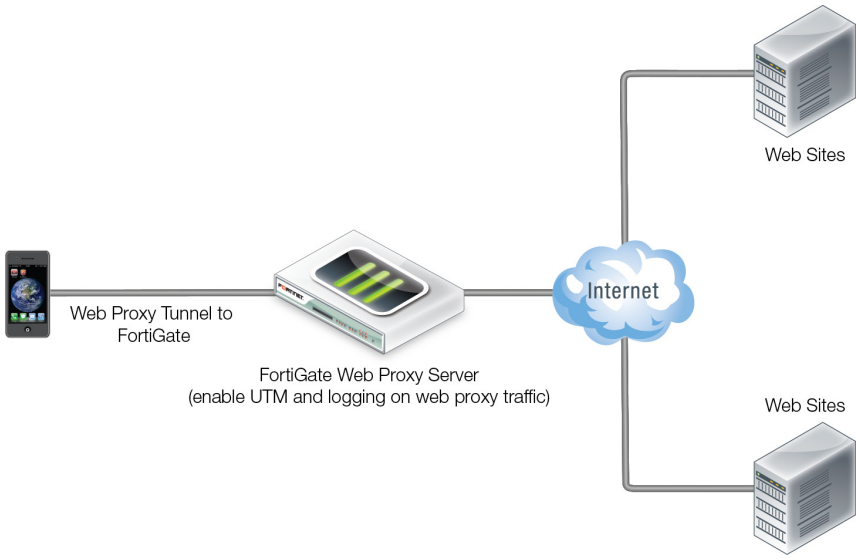
Figure 2: IPsec configuration example



Example 2: Configure your FortiGate as a web proxy server

iOS 6 or later supports *Global Network Proxy* for HTTP. These settings will only affect supervised devices. When this payload is configured and installed on your iOS device, it routes all web traffic from the device through a specified proxy server. This feature is only available when configuring your configuration profile via the Apple Configurator app and the Lion Server *Profile Manager*.

Figure 3: Web proxy configuration example



You can enable FortiGate UTM filtering and logging for FortiClient iOS web traffic when the web proxy feature is implemented. See the *FortiOS 5.0 Handbook* for more information on configuring your FortiGate as a web proxy server for FortiClient iOS web traffic.

You can configure iOS configuration profiles using one of the following utilities:

- iPhone Configuration Utility (Microsoft Windows and Mac OS X operating systems)
- Apple Configurator app (Mac OS X only)
- Profile Manager (Mac Lion Server).

iPhone Configuration Utility

The iPhone Configuration Utility is available from Apple for both Microsoft Windows and Mac OS X operating systems. You can use this utility to create, maintain and encrypt configuration profiles, track and install provisioning profiles, and authorized applications.

The iPhone Configuration Utility is available for download at the following links:

Microsoft Windows

Download the iPhone Configuration Utility 3.6.2 for Microsoft Windows XP SP3, Windows Vista SP1, Windows 7, and Windows 8 at the following link: http://support.apple.com/kb/dl1466.

Mac OS X

Download the iPhone Configuration Utility 3.5 for Mac OS X v10.6 Snow Leopard or later at the following link: http://support.apple.com/kb/dl1465.

For information and support on configuring iPhone for enterprise environments, go to http://www.apple.com/support/iphone/enterprise/. For iPhone Configuration Utility support go to http://help.apple.com/iosdeployment-ipcu/win/1.2/.

Apple Configurator app

The Apple Configurator app is available from the Mac App Store for Mac OS X only. This app allows you to perform the same functions as the iPhone Configuration Utility and also allows you to prepare, supervise, and assign supervised devices to specific users in your organization. To download and install the Apple Configurator you need a Mac computer running OS X v10.65 Snow Leopard or later.

When configuring supervised iOS devices the device will be updated to the latest iOS version, (all data will be erased before installing), the backup cannot be restored, and the supervised devices can only be configured by Apple Configurator on the Mac OS X computer used to prepare the devices. The *supervise* feature is intended for iOS devices that you want to control and configure on an ongoing basis.

For information and support on mass configuration for iOS devices using the Apple Configurator go to http://help.apple.com/configurator/mac/1.2/.

The *Global HTTP Proxy* payload can only be configured using the Apple Configurator App or Lion Server Profile Manager. These settings will only affect supervised devices running iOS 6 or later.

See the *FortiOS 5.0 Handbook* for more information on configuring IPsec VPN and web proxy server on your FortiOS device.

Product Integration and Support

FortiOS support

This feature is supported by FortiOS v5.0 Patch Release 2 or later.

FortiClient iOS support

This feature is supported by FortiClient iOS v5.0 Patch Release 1 or later.

iOS model support

This feature is supported by iOS v5.1.1 or later for the following models:

- iPad: all models
- iPhone: iPhone 4, 4S, 5, 5C, and 5S
- iPod Touch: iPod Touch 3rd generation or later

The *Global HTTP Proxy* settings will only affect supervised devices running iOS 6 or later. This feature can only be configured using the Apple Configurator App for OS X v10.75 Lion or Lion Server Profile Manager.

Option 1: iPhone Configuration Utility

Use the iPhone Configuration Utility to create configuration profiles. The following instructions will guide you through the process of creating a configuration profile (*General* and *VPN* payload) with a Cisco VPN connection to your FortiGate device. You can optionally select to further restrict your iPhone devices by configuring additional payloads.

Configuration profiles

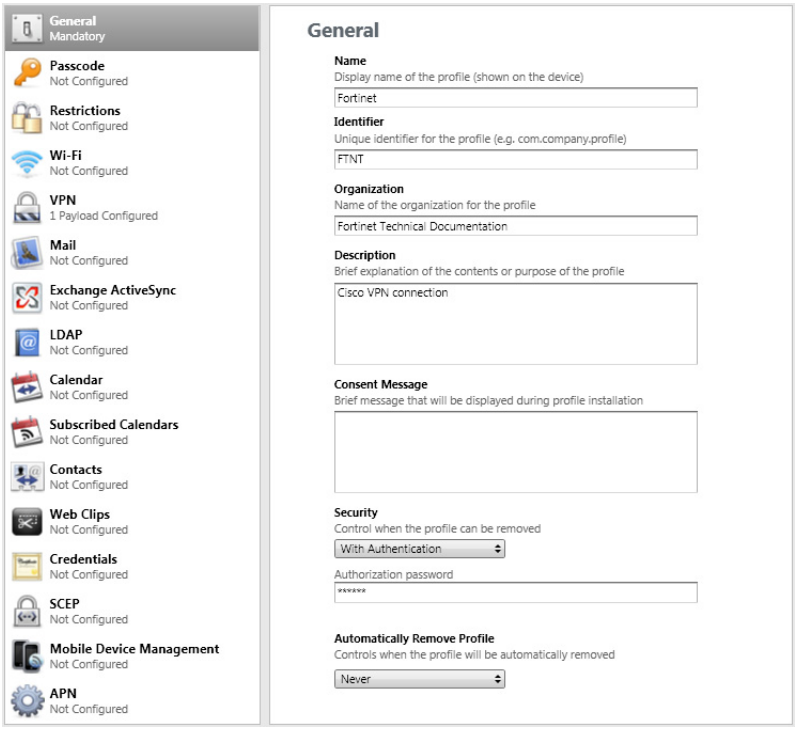
Use the iPhone Configuration Utility to configure the following payloads: *General*, *Passcode*, *Restrictions*, *Wi-Fi*, *VPN*, *Mail*, *Exchange ActiveSync*, *LDAP*, *Calendar*, *Subscribed Calendars*, *Contacts*, *Web Clips*, *Credentials*, *SCEP*, *Mobile Device Management*, and *APN*. For more information on the available payloads, see the *iPhone Configuration Utility* online help available at http://help.apple.com/iosdeployment-ipcu/win/1.2/.

In this example, we will use the iPhone Configuration Utility to configure an IPsec VPN connection to your FortiGate device using the built-in Cisco VPN utility on your iOS device.

To create a configuration profile:

1. Launch the iPhone Configuration Utility.
2. Select *Configuration Profiles* in the left tree menu.
3. Select *New* in the top menu bar to create a configuration profile.
4. Select *General* in the content pane. The *General* payload is mandatory.

Figure 4: General payload window

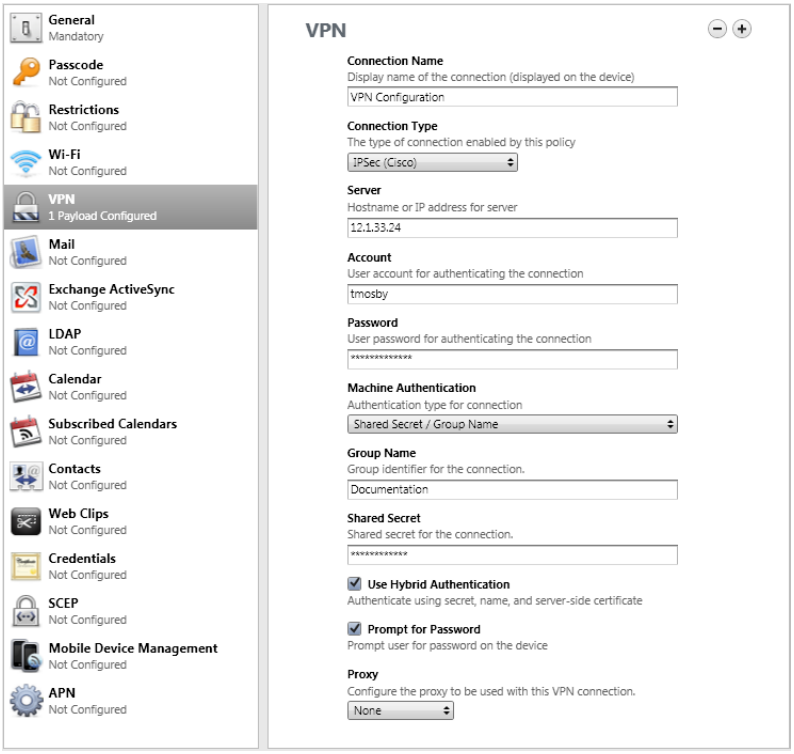


5. Configure the following settings:

Name	Enter the name of the profile.
Identifier	Enter a unique identifier for the profile.
Organization	Enter the name of the organization for the profile.
Description	Enter a brief explanation of the contents or purpose of the profile (optional).
Consent Message	Enter a brief message that will be displayed during profile installation.
Security	Select to control when the profile can be removed. Select one of the following: *Always*, *With Authentication*, or *Never*.
Automatically Remove Profile	Select to control when the profile will be automatically removed. Select one of the following: *Never*, *On Date (select the date)*, or *After Interval (select the interval value)*.

6. Select *VPN* in the content pane and select *Configure* to create a VPN payload. Configure your Cisco VPN settings to connect to your FortiGate device.

Figure 5: VPN payload window



7. Configure the following settings:

- / +	Select to delete or add a VPN configuration.
Connection Name	Enter the name of the VPN connection.
Connection Type	Enter the type of connection enabled by this policy. Select *IPSec (Cisco)* in the drop-down menu.
Server	Enter the hostname or IP address of the FortiGate device.
Account	Enter the user account for the connection.
Password	Enter the password associated with the user.

Machine Authentication	Enter the authentication type for the connection. Select one of the following:
	• *Certificate*
	When selecting Certificate, you must configure credentials in the Credentials payload:
	  • *Include User PIN*: Select to request a PIN during connection and send with authentication.
	  • *Enable VPN On Demand*: Select to add domains and host names that will establish a VPN.
	• *Shared Secret / Group Name*
	  • *Group Name*: Enter a group name identifier for the connection
	  • *Shared Secret*: Enter a shared secret for the connection.
	  • *Use Hybrid Authentication*: Select to authenticate user secret, name, and server-side certificate.
	  • *Prompt for Password*: Select to prompt user for password on the device.

Proxy	Configure the proxy to be used with this VPN connection. Select one of the following:
	• *None*
	• *Manual*
	  • *Server and Port*: Enter the fully qualified address and port of the proxy server.
	  • *Authentication*: Enter the username used to connect to the proxy server.
	  • *Password*: Enter the password used when connecting to the proxy server.
	• *Automatic*
	  • *Proxy Server URL*: Enter the server to get proxy settings from.

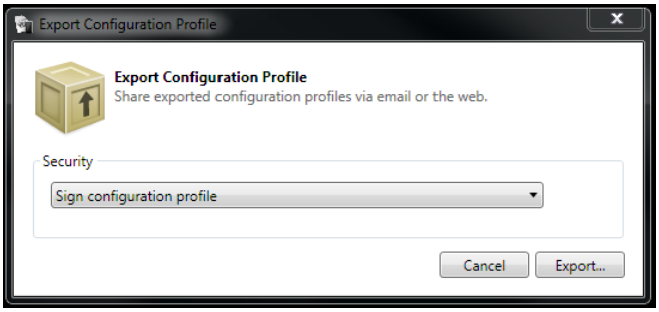
FortiClient iOS requires Safari to install the `.mobileconfig` profile. As such, the *Allow Use of Safari* option under *Restrictions* > *Applications* must be enabled.

You can use the *Restrictions* payload to restrict device functionality, enable access to applications on the device, enable access to iCloud services, enforce security and privacy policies, control access to apps and media, set the region for ratings, and set the maximum allowed ratings.

For information on configuring certificates, see the *Provision Certificates to iOS Devices Technical Note*.

8. Select *Export* in the title bar to export the configuration profile.

Figure 6: Export configuration profile window



9. Select *Export* in the *Export Configuration Profile* window. Save the `.mobileconfig` file to your local computer.

Select *Sign configuration profile* in the drop-down menu to use *the iPhone Configuration Utility's cer*tificate to sign the profile. When a profile is signed, recipients can determine who signed the profile and whether or not the profile has been modified since it was signed.

Option 2: Apple Configurator App

Use the Apple Configurator app to create configuration profiles, update devices, and create device groups. The following instructions will guide you through the process of creating a configuration profile (*General*, *VPN* payload, and Global HTTP Proxy payload) with a Cisco VPN connection to your FortiGate device, and use your FortiGate as a web proxy server.You can optionally select to further restrict your iPhone devices by configuring additional payloads.

Figure 7: Welcome page

The Apple Configurator app includes a *Global HTTP Proxy* payload which is not available on the iPhone Configuration Utility. Use this payload to specify a proxy for all HTTP traffic to an from the iOS 6 device.

Configuration profiles

Use the Apple Configurator app to configure the following payloads: *General*, *Passcode*, *Restrictions*, *Global HTTP Proxy*, *Wi-Fi*, *VPN*, *Mail*, *Exchange ActiveSync*, *Calendar*, *Contacts*, *Subscribed Calendar, Web Clips*, *Credentials*, *SCEP*, and *APN*. For more information on the available payloads, see the *Apple Configurator Help Mass configuration for iOS devices* online help available at http://help.apple.com/configurator/mac/1.2/.

Only supervised iOS devices can install a mobile configuration with the *Global HTTP* proxy payload. When supervising iOS devices, the device will be upgraded to the latest iOS version and set to default values. The exported file as the syntax `HTTP_proxy.mobileconfig`.

When supervising devices with Apple Configurator, you can install free apps, paid apps using VPP codes, enterprise apps, and documents. Before you can install apps (including FortiClient), you need to add them to Apple Configurator.

A `.mobileconfig` profile created using the iPhone Configuration Utility can be imported into the Apple Configurator app. The iPhone Configuration Utility does not have an import function.

When supervision is enabled, you must configure the *Restrictions* payload and select to A*llow Configuration Profile Installation* to allow the iOS device to receive configuration profiles from your FortiOS device.

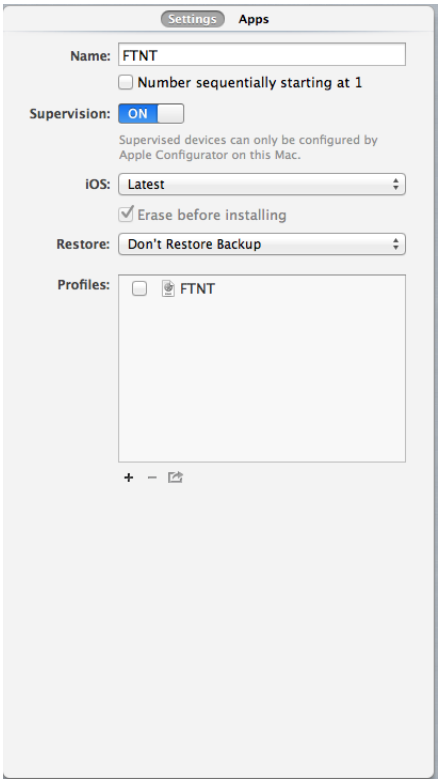
When changing the device status from *Supervise* to *Unsupervise*, the device is set to factory default settings and needs to be set up again.

In this example, we will configure a configuration profile (*General*, *VPN* payload, and Global HTTP Proxy payload) with a Cisco VPN connection to your FortiGate device, and use your FortiGate as a web proxy server for mobile internet traffic.

To create a configuration profile:

1. Launch the Apple Configurator app in Launchpad.
2. Select the *Start Preparing Devices* icon in the bottom toolbar and create a new *Apple Configurator* profile.

Figure 8: Prepare window

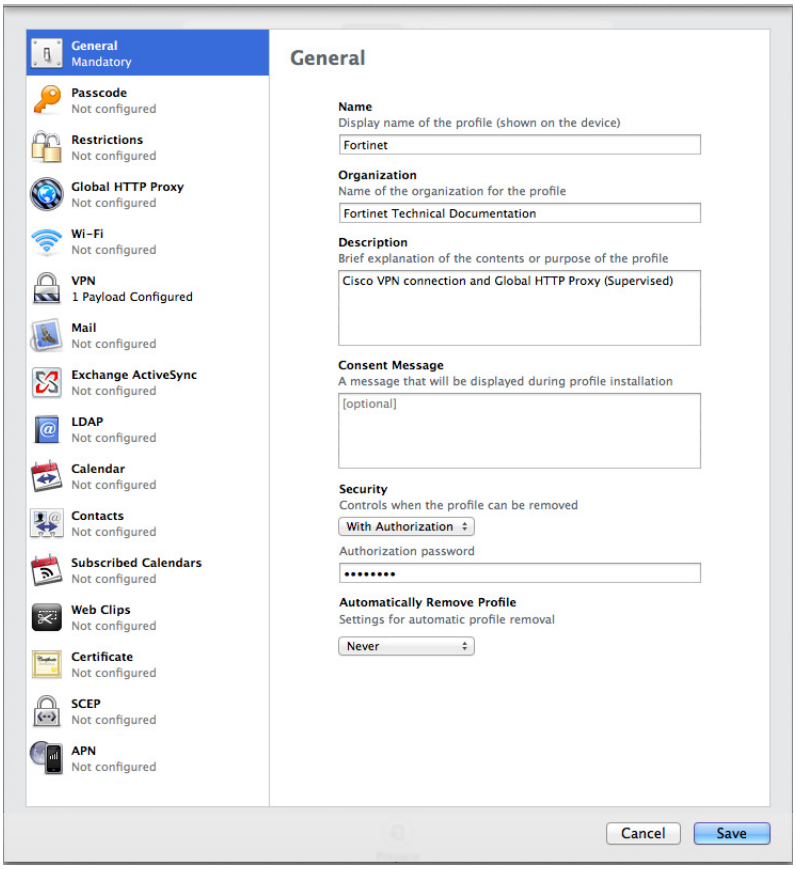


3. In the *Settings* page configure the following:

Name	Enter a name for the Apple Configurator profile. Select the checkbox to number sequentially starting at 1.
Supervision	Toggle the switch *ON* or *OFF* for supervision mode. Supervised devices can only be configured by Apple Configurator on the Mac computer.
iOS	When supervision is disabled, you can select to keep the device at the current iOS version, install the latest iOS version, or install an earlier version downloaded from the Apple site. When supervision is enabled, you can select to install the latest iOS version or install an earlier version downloaded from the Apple site. Note that the device will be erased before installing.
Restore	When supervision is disabled, you can select to restore the backup or not to restore the backup. When supervision is enabled, you can not restore the backup.
Profiles	List of configuration profiles. Select the plus (+) icon to create a profile, select the minus (-) icon to delete a profile, or select the export configuration profile icon to export the profile to your local computer.

4. Select the plus (+) icon and select *Create New Profile* in the drop-down menu to create a configuration profile.
5. Select *General* in the content pane. The *General* payload is mandatory.

Figure 9: General payload window

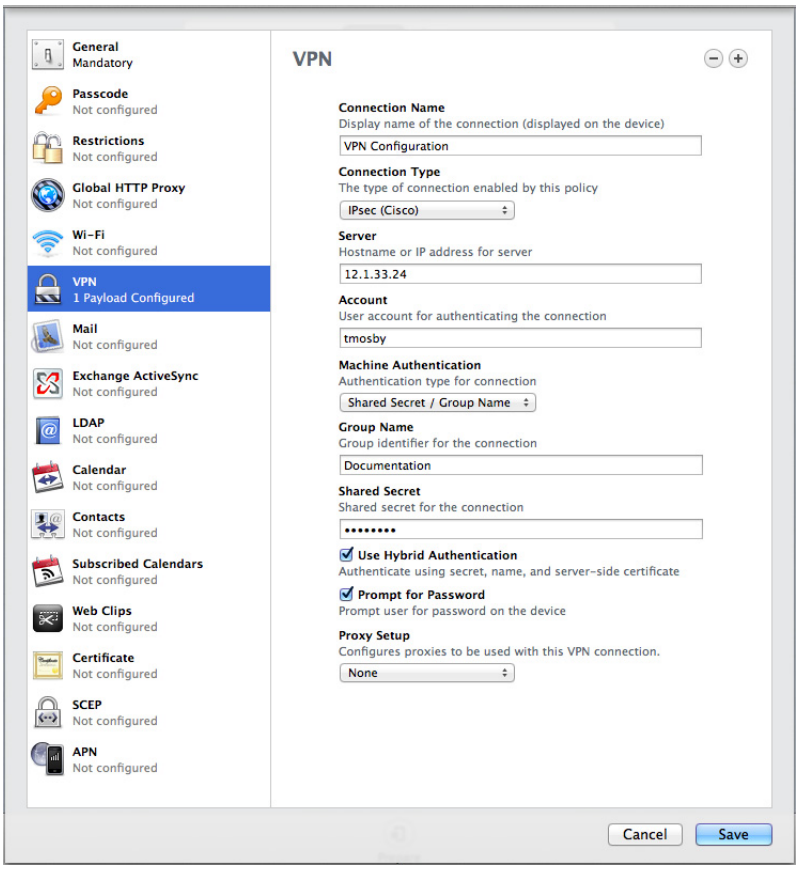


6. Configure the following settings:

Name	Enter the name of the profile.
Organization	Enter the name of the organization for the profile.
Description	Enter a brief explanation of the contents or purpose of the profile. (optional)
Consent Message	Enter a brief message that will be displayed during profile installation.
Security	Select to control when the profile can be removed. Select one of the following: *Always*, *With Authorization*, or *Never*.
Automatically Remove Profile	Select to control when the profile will be automatically removed. Select one of the following: *Never*, *On Date (select the date)*, or *After Interval (select the interval value)*.

7. Select *VPN* in the content pane and select *Configure* to create a VPN payload. Configure your Cisco VPN settings to connect to your FortiGate device.

Figure 10:VPN payload window



8. Configure the following settings:

- / +	Select to delete or add a VPN configuration.
Connection Name	Enter the name of the VPN connection.
Connection Type	Enter the type of connection enabled by this policy. Select *IPsec (Cisco)* in the drop-down menu.
Server	Enter the hostname or IP address of the FortiGate device.
Account	Enter the user account for the connection.
Password	Enter the password associated with the user.

Machine Authentication	Enter the authentication type for the connection. Select one of the following:
	• *Certificate*
	When selecting Certificate, you must configure credentials in the Credentials payload.
	  • *Include User PIN*: Select to request a PIN during connection and send with authentication.
	  • *Enable VPN On Demand*: Select to add domains and host names that will establish a VPN.
	• *Shared Secret / Group Name*
	  • *Group Name*: Enter a group name identifier for the connection
	  • *Shared Secret*: Enter a shared secret for the connection.
	  • *Use Hybrid Authentication*: Select to authenticate user secret, name, and server-side certificate.
	  • *Prompt for Password*: Select to prompt user for password on the device.

Proxy	Configure the proxy to be used with this VPN connection. Select one of the following:
	• *None*
	• *Manual*
	  • *Server and Port*: Enter the fully qualified address and port of the proxy server.
	  • *Authentication*: Enter the username used to connect to the proxy server.
	  • *Password*: Enter the password used when connecting to the proxy server.
	• *Automatic*
	  • *Proxy Server URL*: Enter the server to get proxy settings from.

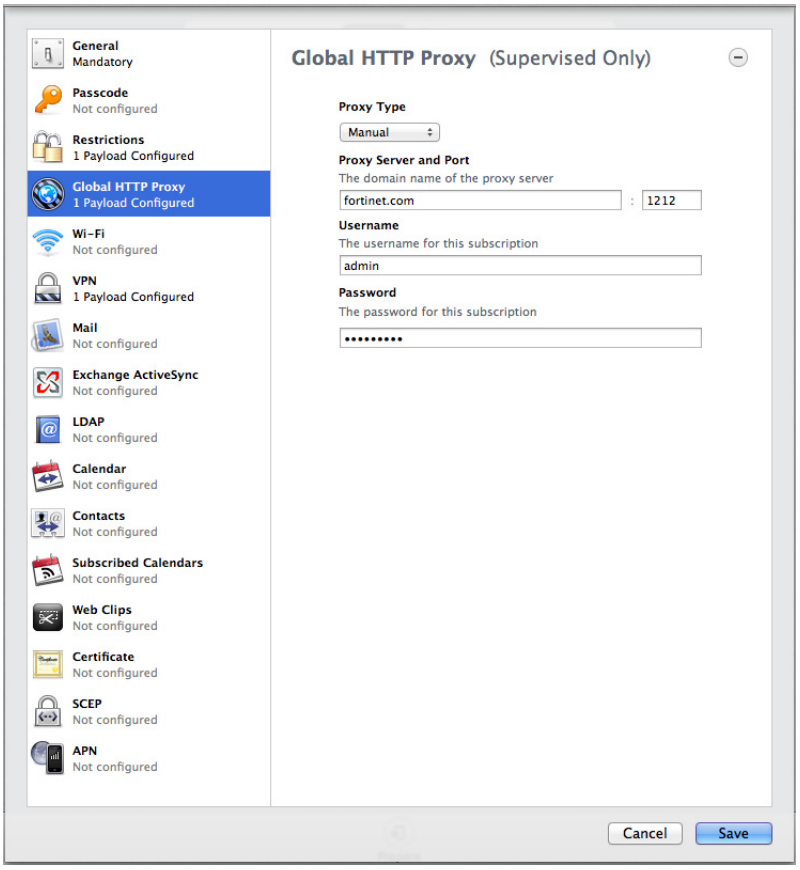
FortiClient iOS requires Safari to install the `.mobileconfig` profile. As such, the *Allow Use of Safari* option under *Restrictions* > *Applications* must be enabled.

You can use the *Restrictions* payload to restrict device functionality, enable access to applications on the device, enable access to iCloud services, enforce security and privacy policies, control access to apps and media, set the region for ratings, and set the maximum allowed ratings.

For information on configuring certificates, see the *Provision Certificates to iOS Devices Technical Note*.

9. Select *Global HTTP Proxy* in the content pane and select *Configure* to create a *Global HTTP Proxy* payload. Your FortiGate can be configured as the global proxy server to provide UTM protection and traffic monitoring to your iOS devices.

Figure 11: Global HTTP Proxy window



10. Configure the following settings:

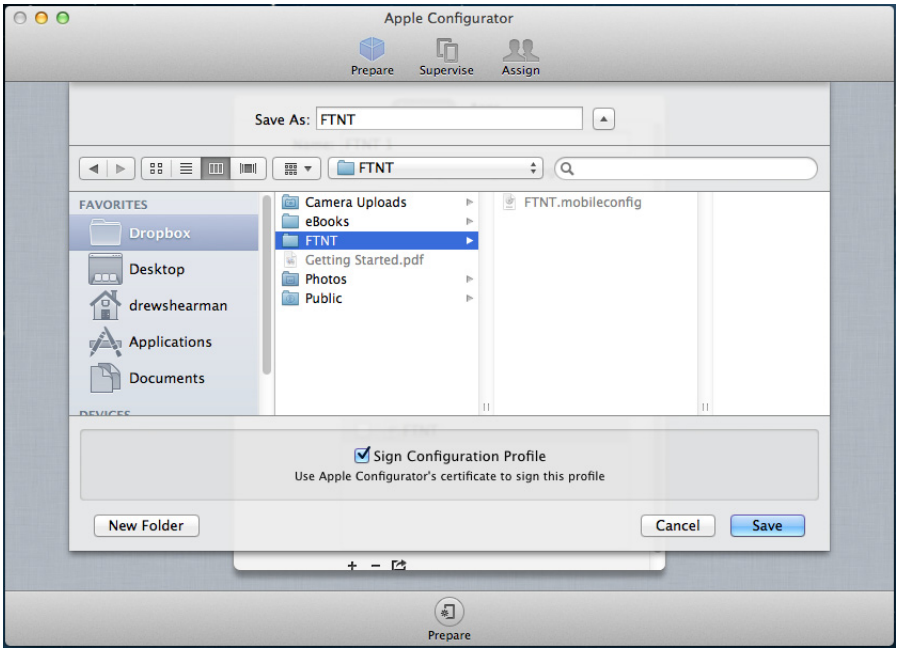
Proxy Type	Select the proxy type in the drop-down menu. Select either *Manual* or *Auto*. When Auto is selected, enter the URL used to retrieve proxy settings.
Proxy Server and Port	When manual proxy is selected, enter the domain name of the proxy server and enter the port number.
Username	When manual proxy is selected, enter the username for this subscription.
Password	When manual proxy is selected, enter the password for this subscription.

11. Select *Save* to save the configuration profile.

12. In the *Prepare* > *Settings* menu, select the *Export Configuration Profile* icon below the list, and then name and save the profile.

Select the checkbox to use the Apple Configurator's certificate to sign the profile. When a profile is signed, recipients can determine who signed the profile and whether or not the profile has been modified since it was signed.

Figure 12: Export configuration profile window



FortiClient iOS Endpoint Management

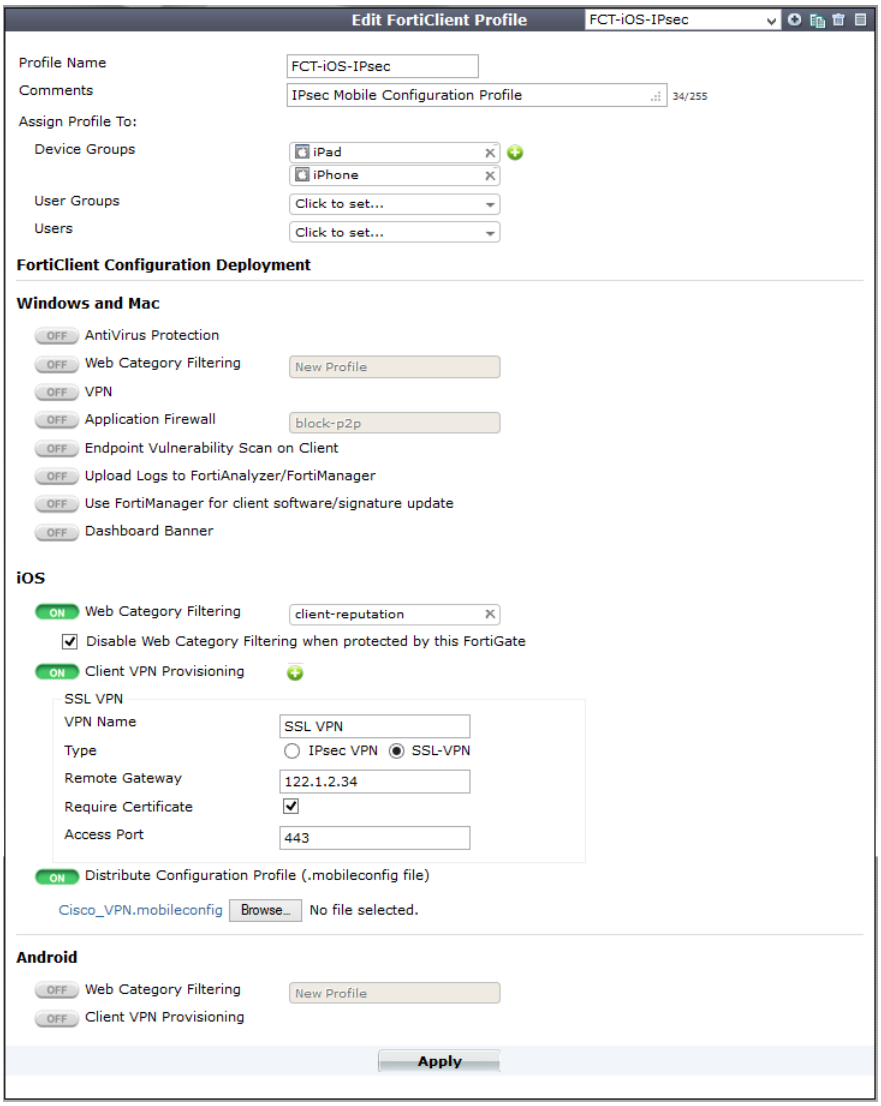
The following instructions will guide you through the process of importing the `.mobileconfig` file into your FortiOS *Endpoint Profile* and installing this profile to registered iOS devices.

To import the .mobileconfig file to your FortiGate device:

1. Go to *User & Device* > *Endpoint Protection* > *FortiClient Profiles*.

   The *Edit FortiClient Profile* window opens.

   Figure 13: Edit FortiClient profile window



2. Under *iOS*, select to enable *Distribute Configuration Profile (.mobileconfig file)*.
3. Select *Browse* and locate the `.mobileconfig` file that you saved to your management computer.

4. Select *Apply* to save the configuration.

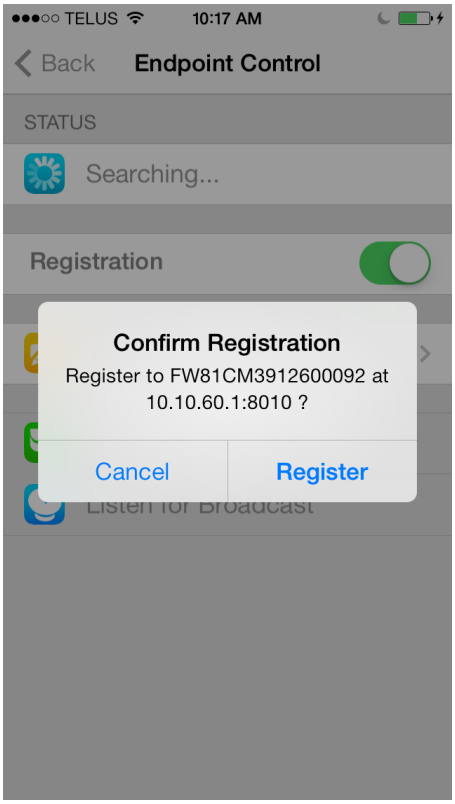
The mobile configuration is pushed to registered client devices.

Install the configuration profile on your FortiClient iOS device:

1. Launch the FortiClient application on your iOS device.
2. Select the options icon in the tool-bar and select *Endpoint Control*.
3. FortiClient will search for the FortiGate device.

   [Alternatively, you can select specify *Preferred Host* and enter the host name or IP and port number.]
4. Select *Register* to register your FortiClient iOS device with the FortiGate.

Figure 14: Confirm registration pop-up window

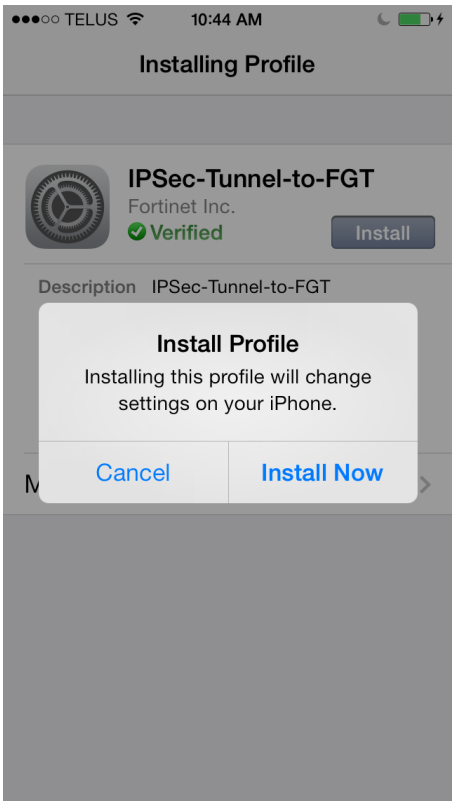


5. FortiClient will launch the *Install Profile* page. Select *Install* to install the configuration profile to your FortiClient iOS device.

Figure 15: Install profile window

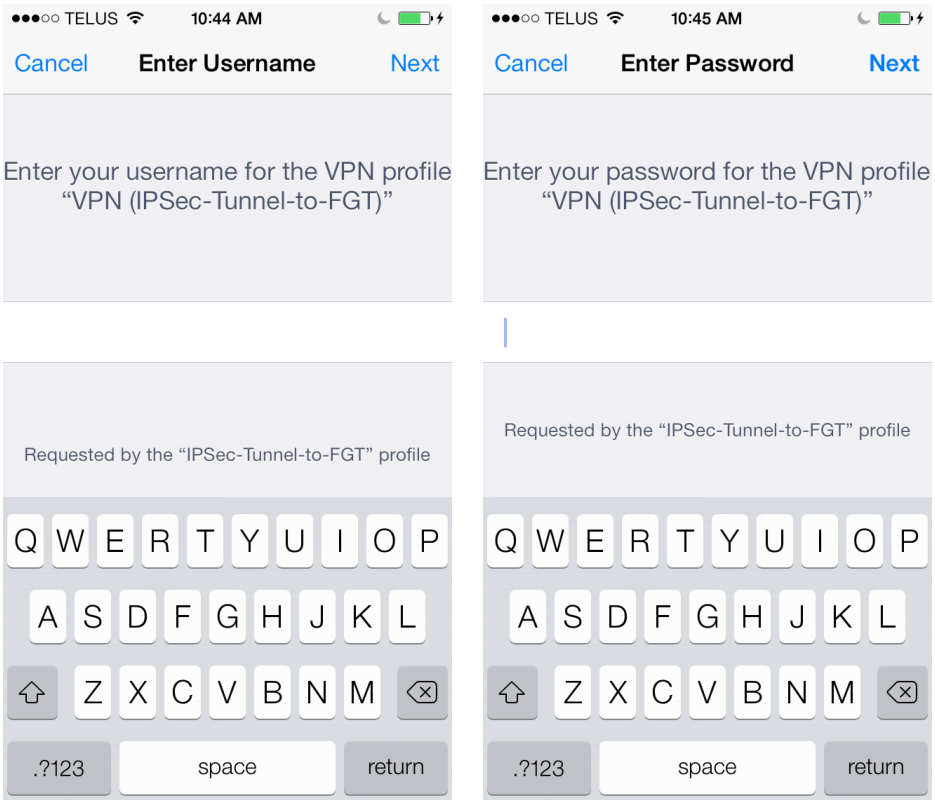
6. Select *Install* to proceed with the installation.

Figure 16: Installing profile window



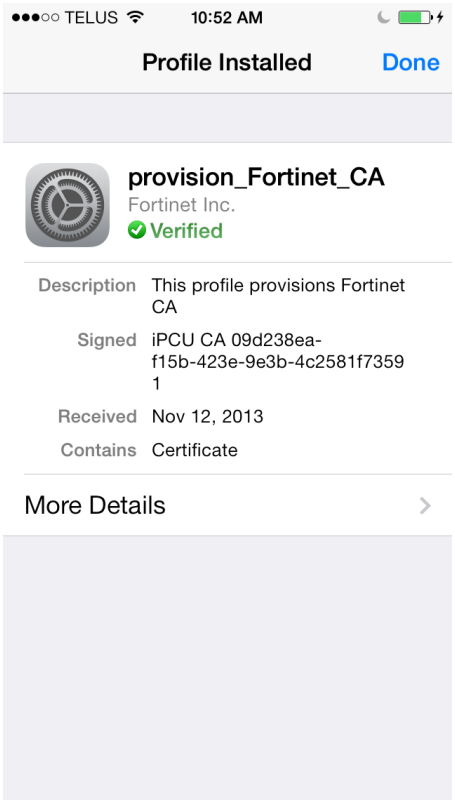
7. Enter your username and password for the VPN connection to the FortiGate.

Figure 17: Username and password windows



A *Profile Installed* confirmation window is displayed.

Figure 18: Profile installed confirmation window



8. Select *Done* to continue. You can now use FortiClient (iOS).